Solutions

Each answer shows the steps, then the **result**.

2.1

- a product ships with its security features already enabled, so it is safe out of the box without the user changing settings

2.2

- SQL injection; XSS; directory traversal

2.3

- control characters such as the single quote, double quote, and semicolon

3.1 B

- input sanitization stops all three input attacks

3.2 B

- security is a design principle throughout development

3.3

(a)

- SQL injection

(b)

- sanitization strips dangerous control characters from the input so they cannot alter the database query